LISTING OF CLAIMS

1.   (currently amended) A method for generating a digital
     signature in a signature device having a signature
     program and certificate with signature key stored
     thereon for the signing of <u>a document, wherein the</u>
     <u>digital signature identifies at least one</u>
     <u>characteristic of said signature device</u> ~~documents~~,
     comprising the steps of:

     a)   receiving input information to said signature
     device; and

     b)   executing said signature program by the steps of:
     creating a signature data set comprising at least the
     received information<u>, at least one identifying</u>
     <u>characteristic to identify said signature device,</u> and a
     document extract value of the document for signing; and
     creating an expanded digital signature by encrypting
     the signature data set with the aid of a signature key
     stored in said certificate.

2.   (previously presented) The method in accordance with Claim 1, wherein said receiving input information comprises procuring the value of a signature counter from said signature device.

3.   (original) The method in accordance with Claim 2, further comprising, prior to said procuring, creating the signature counter as an attribute of the signature key.

4.   (currently amended) The method in accordance with Claim 1 wherein the receiving input information comprises procuring the ~~an~~ identifying characteristic to identify the signature device from said signature device.

5.   (currently amended) The method in accordance with Claim 1 ~~4~~, wherein the receiving input information comprises procuring information as to the hardware and software environment used in creating the digital signature.

6.   (original) The method in accordance with Claim 1, further comprising entering an identifying

characteristic to identify the holder of the signature key prior to said receiving input information.

7. (original) The method in accordance with Claim 6, further comprising creating the identifying characteristic to identify the holder of the signature key as an attribute of the signature key.

8. (original) The method in accordance with Claim 7, further comprising changing the identifying characteristic to identify the holder of the signature key prior to said receiving.

9. (currently amended) ~~A self-authenticating~~ An electronic signature device for generating a digital signature to sign a document comprising:

a) a receiver for receiving input information;

b) at least one storage location for storing at least a signature program and a certificate with signature key;

c) a data processor component for _executing said_ _signature program comprising at least a component for_ creating a signature data set comprising at least the received information_, at least one identifying_ _characteristic identifying the signature device,_ and a document extract value of the document for signing; and

e) an encryption component for creating an expanded digital signature by encrypting the signature data set with the aid of a signature key stored at said signature device.

10. (original) The signature device in accordance with Claim 9, wherein the device is a chipcard.

11. (currently amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for generating a digital signature _to sign_ _a document_ in a ~~self-authenticating~~ signature device having a signature program and certificate with signature key stored thereon, said method steps comprising:

a)   receiving input information to said signature device; and

b)   executing said signature program by the steps of: creating a signature data set comprising at least the received information, at least one identifying characteristic for identifying said signature device, and a document extract value of the document for signing; and creating an expanded digital signature by encrypting the signature data set with the aid of a signature key stored in said certificate.

12.   (currently amended) An improved digital signature, wherein the improvement comprises the inclusion of additional information generated by a self-authenticating signature device having signature certificate information stored with a signature program, said additional information identifying the signature device, in addition to a document extract value of a document for signing.

13.   (original) The improvement in accordance with Claim 12,
      wherein the additional information comprises
      information which uniquely identifies it in relation to
      every other digital signature generated with the same
      signature key.

14.   (canceled)

15.   (original) The improvement in accordance with Claim 12
      wherein the additional information comprises
      information on the hardware and software environment
      used in generating the signature.